Dokumentácia riešenia

**SOS**

**Skupina 5 Meno a priezvisko:**

**Radovan Kyjak,**

**Radovan Kohutiar**

**Preambula / Účel**

Účelom tohto dokumentu je poskytnúť informácie o riešení SOS.

|  |  |
| --- | --- |
| Dokument: | Dokumentácia riešenia **SOS** |
| Verzia: | 1.0 |
| Autor: | Radovan Kyjak, Radovan Kohutiar |

**História dokumentu**

|  |  |  |
| --- | --- | --- |
| Verzia | Dátum verzie | Popis zmien |
| 0.01 | 11.9.2017 | Úvodný draft |
| 0.1 | 3.10.2017 | Linux – Firewall, DHCP |
| 0.2 | 10.10.2017 | Linux - DNS |
| 0.3 | 17.10.2017 | Linux – DNS, Apache |
| 0.4 | 24.10.2017 | Linux - NTP |
| 0.5 | 31.10.2017 | Linux - Mail |
| 0.6 | 7.11.2017 | Linux – syslog-ng |
| 0.7 | 21.11.2017 | Windows – DHCP, NTP |
| 0.8 | 28.11.2017 | Windows - DNS |
| 0.9 | 12.12.2017 | Windows - ISS |
| 1.0 | 21.12.2017 | Finálna verzia |
|  |  |  |

# Obsah

[1 Obsah 4](#_Toc501655540)

[2 Zoznam tabuliek 5](#_Toc501655541)

[3 Zoznam obrázkov 6](#_Toc501655542)

[4 Úvod 8](#_Toc501655543)

[1 Linux 9](#_Toc501655544)

[1.1 Topológia zapojenia 9](#_Toc501655545)

[1.2 Základná konfigurácia 10](#_Toc501655546)

[1.3 Firewall 12](#_Toc501655547)

[1.4 DHCP 16](#_Toc501655548)

[1.5 DNS 20](#_Toc501655549)

[1.6 APACHE 25](#_Toc501655550)

[1.7 NTP 28](#_Toc501655551)

[1.8 Mail 31](#_Toc501655552)

[1.9 Syslog 32](#_Toc501655553)

[2 Windows 35](#_Toc501655554)

[2.1 Topológia zapojenia 35](#_Toc501655555)

[2.2 Základná konfigurácia 35](#_Toc501655556)

[2.3 DHCP 37](#_Toc501655557)

[2.4 DNS 40](#_Toc501655558)

[2.5 NTP 45](#_Toc501655559)

[2.6 IIS – Internet Information Server 46](#_Toc501655560)

[3 Záver 49](#_Toc501655561)



# Zoznam tabuliek

[*Tabuľka 1 Adresný plan Linux* 8](#_Toc501648107)

[*Tabuľka 2 Adresný plan Windows* 34](#_Toc501648108)

# Zoznam obrázkov

[Obrázok 1 interfaces 10](#_Toc501655497)

[Obrázok 2 firewall - zakladny 13](#_Toc501655498)

[Obrázok 3 firewall - ICMP, DHCP, SSH, APACHE 14](#_Toc501655499)

[Obrázok 4 firewall - NAT, SSH tunely, DNS 15](#_Toc501655500)

[Obrázok 5 firewall - NTP, syslog, Mail 15](#_Toc501655501)

[Obrázok 6 dhcp.d 16](#_Toc501655502)

[Obrázok 7 isc-dhcp-relay 17](#_Toc501655503)

[Obrázok 8 statická IP adresa 18](#_Toc501655504)

[Obrázok 9 nastavenie klienta na DHCP 19](#_Toc501655505)

[Obrázok 10 DNS - named.conf.options 20](#_Toc501655506)

[Obrázok 11 DNS - named.conf.local 21](#_Toc501655507)

[Obrázok 12 DNS - named.conf.default-zones 22](#_Toc501655508)

[Obrázok 13 DNS - zónový súbor pre lokálnu časť siete 22](#_Toc501655509)

[Obrázok 14 DNS - súbor 168.192 23](#_Toc501655510)

[Obrázok 15 DNS - zónový súbor pre verejnú časť siete 23](#_Toc501655511)

[Obrázok 16 DNS - súbor 168.192 pre verejnú časť siete 23](#_Toc501655512)

[Obrázok 17 DNS - slave named.conf.local 24](#_Toc501655513)

[Obrázok 18 Apache – virtual host súbor 25](#_Toc501655514)

[Obrázok 19 Apache – virtual host súbor 26](#_Toc501655515)

[Obrázok 20 interné DNS 27](#_Toc501655516)

[Obrázok 21 externé DNS 27](#_Toc501655517)

[Obrázok 22 NTP - kofigurácia serveru 28](#_Toc501655518)

[Obrázok 23 NTP - konfigurácia klienta 29](#_Toc501655519)

[Obrázok 24 NTP - úspešná synchronizácia 30](#_Toc501655520)

[Obrázok 25 syslog-ng.conf 32](#_Toc501655521)

[Obrázok 26 collector 32](#_Toc501655522)

[Obrázok 27 s\_net 33](#_Toc501655523)

[Obrázok 28 s\_src 33](#_Toc501655524)

[Obrázok 29 d\_tcp 34](#_Toc501655525)

[Obrázok 30 zmena hesla Windows 36](#_Toc501655526)

[Obrázok 31 Pridanie viacerých IP adries Windows 37](#_Toc501655527)

[Obrázok 32 DHCP rozsah Windows 39](#_Toc501655528)

[Obrázok 33 System 40](#_Toc501655529)

[Obrázok 34 DNS suffix Windows 41](#_Toc501655530)

[Obrázok 35 DNS Windows 42](#_Toc501655531)

[Obrázok 36 New host 42](#_Toc501655532)

[Obrázok 37 New pointer 43](#_Toc501655533)

[Obrázok 38 Edit name server record 44](#_Toc501655534)

[Obrázok 39 regedit NTP 45](#_Toc501655535)

[Obrázok 40 Add roles and features 46](#_Toc501655536)

[Obrázok 41 interný new host 47](#_Toc501655537)

[Obrázok 42 interné DNS 48](#_Toc501655538)

[Obrázok 43 externé DNS 48](#_Toc501655539)

# Úvod

Dokument popisuje systémovú architektúru riešenia SOS v akademickom roku 2017/18, ktorá pozostáva z viacerých virtuálnych zariadení a obsahuje konfiguračné postupy implementácie požadovaných služieb.

# Linux

## **Topológia zapojenia**

Topológia SOS sa skladá z routera, dvoch serverov a klienta.

|  |  |  |  |
| --- | --- | --- | --- |
| Názov zariadenia | Rozhranie | IP adresa | Popis |
| Server-router | ens3  ens3  ens4  ens5 | 158.193.153.149  158.193.153.153  192.168.1.1  192.168.2.1 | Linux router |
| Server1 | ens3 | 192.168.1.2 | OS Debian server |
| Server2 | ens3 | 192.168.1.3 | OS Debian server |
| Klient | ens3 | DHCP | Linux desktop |

Tabuľka 1 Adresný plan Linux

Malá podniková sieť bude pripojená Linux smerovačom s aplikovaným netfilter firewallom a NAT na poskytovateľa verejnej konektivity. V našom prostredí je ISP LAN sieť cloud-u s IPv4 verejným rozsahom 158.193.153.0/24. Z tohto priestoru získaj každý tím dve verejné IP adresy (viď časť DNS dole). Sieť podniku má pridelenú vlastnú DNS zónu, aby bolo možné realizovať vkladanie DNS záznamov vo vlastnej réžii. Pre tento účel bola na DNS serveri ISP vykonaná delegácia DNS zón na študentské DNS servery. Zóny sú tvorené pre potreby cvičenia v DNS priestore cloud-u ".cc.uniza.sk". Ich tvar je per skupinu:

1. ns1.sos5.cc.uniza.sk: 158.193.153.149
2. ns2.sos5.cc.uniza.sk: 158.193.153.153

## **Základná konfigurácia**

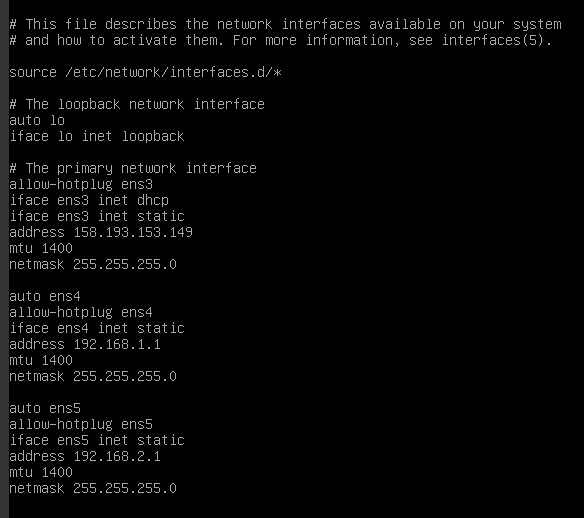
Základná konfigurácia zahŕňa vytvorenie nových používateľov, zmenu ich prihlasovacích údajov a nastavenie adries rozhraniam.

Vymazanie defaultného cloud usera sme vykonali pomocou spustenia nasledujúceho príkazu ako root: deluser --remove-home cloud.

Pridanie nového účtu sme vykonali pomocou spustenia nasledujúceho príkazu ako root: adduser MENO. Počas nastavovania hodnôt pre nový účet systém ponúkne možnosť zmeny viacerých nastavení. Vybrali sme defaultné hodnoty, zmenili sme len heslo.

Po vytvorení nových prihlasovacích údajov sme prešli k nastaveniu rozhraní. Tieto zmeny boli vykonané v súbore /etc/network/interfaces. Zmeny boli vytvorené podľa potrieb každého zariadenia.

Na nasledujúcom obrázku je znázornený aktuálny stav tohoto súboru pre stroj server-router.



Obrázok 1 interfaces

Pre rozhranie ens3 smerujúce do internetu môžeme vidieť pridanie druhej potrebnej IP adresy podľa zadania. Pre rozhrania ens4 a ens5 môžeme vidieť nastavenie statických IP adries pre lokálne siete, nakoľko tieto rozhrania slúžia ako default gateway pre stroje v sieťach.

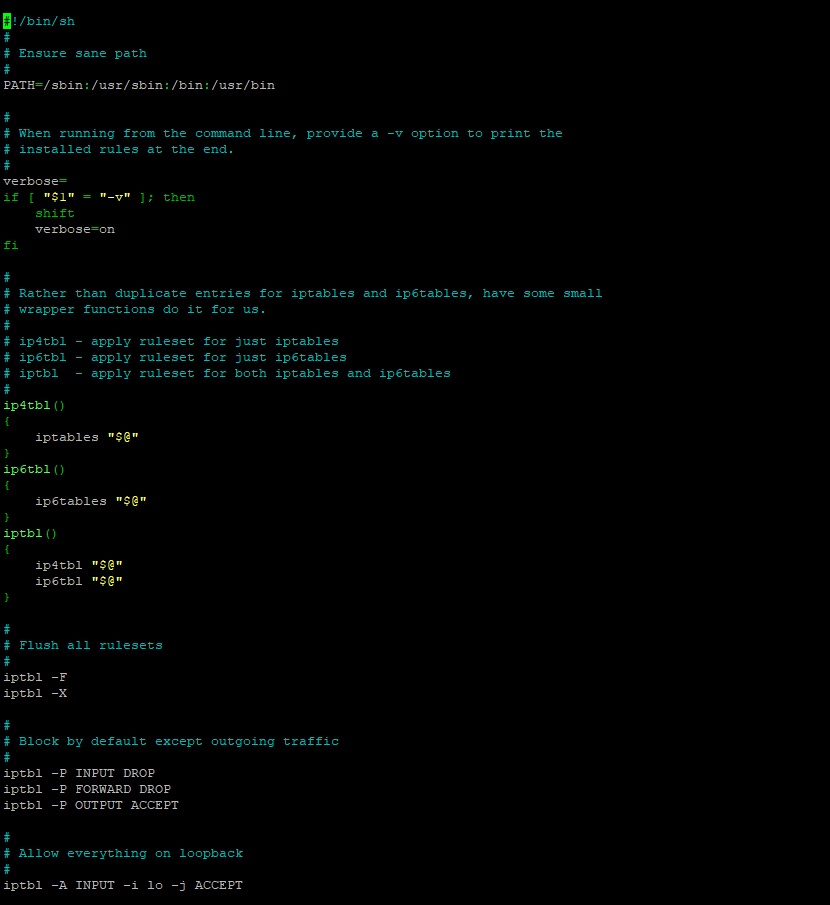
Týmto bola vykonaná základná konfigurácia.

## **Firewall**

Vytvorili sme skript s názvom ipTablesScript.sh, ktorý sme umiestnili do priečinku /etc/init.d/. Tento skript obsahuje záznamy pravidiel iptables pre povolenie a zakázanie dátovej prevádzky cez našu sieť. Nastavili sme práva pre spúšťanie daného skriptu pomocou príkazu chmod 744 /etc/init.d/iptablesScript.sh a nastavili sme jeho spúšťanie pri štarte pomocou programu crontab. Po prihlásení ako root sme zadali príkaz crontab –e, ktorý nám otvoril konfiguračný súbor, kde sme pridali nasledovný riadok: @reboot /etc/init.d/ipTablesScript.sh. Tento riadok zabezpečí štart skriptu pri štarte alebo reštarte systému.

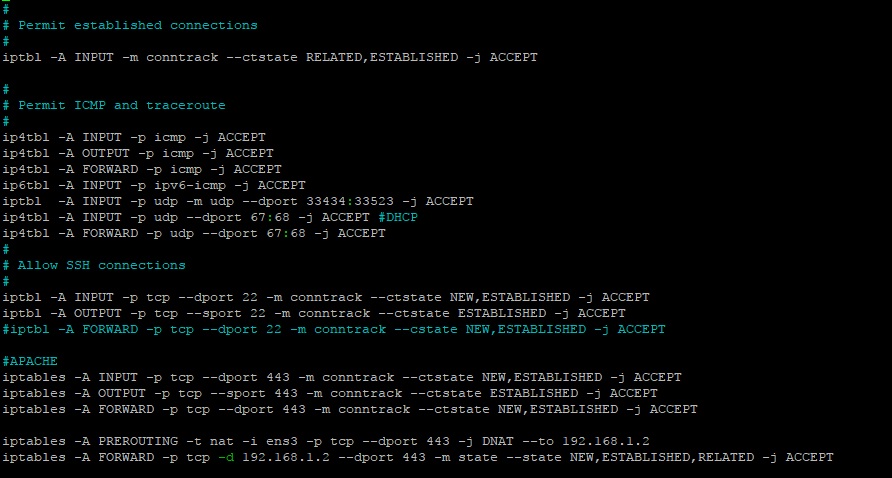
Skript pre stroj server-router vyzerá nasledovne (skript bol pridaný aj pre všetky ostatné zariadenia, každý stroj v ňom avšak obsahuje mierne zmeny podľa potrieb):

V prvom rade nastavujeme defaultné hodnoty, čiže flushujeme všetky pravidlá v sekcii Flush all rulesets. Toto spôsobí vymazanie všetkých existujúcich pravidiel a následne v sekcii Block by default except outgoing traffic nastavujeme pravidlá pre zahodenie prichádzajúcej prevádzky a povolujeme len odchádzajúce pakety. Tieto príkazy môžeme vidieť na obrázku 2.



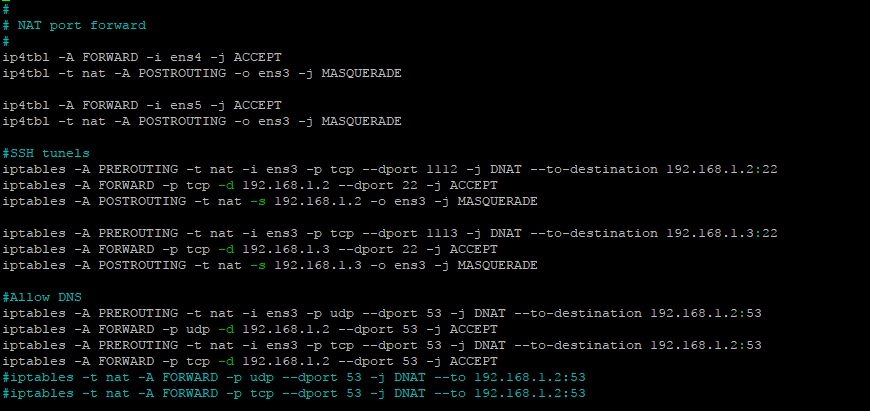
Obrázok 2 firewall - zakladny

Na obrázku 3v sekcii Permit ICMP and traceroute vidíme povolenie pingov, traceroute a povolenie UDP portov 67 a 68, ktoré slúžia na prenos DHCP requestov po sieti. V sekcii Allow SSH connections vidíme povolenie TCP portu 22, ktorý slúži na vzdialené pripojenie pomocou SSH. Sekcia APACHE slúži na povolenie TCP portu 443, ktorý slúži na pripojenie na náš webserver. Tento skript sa ale nachádza na stroji server-router a tak je potrebné dané pripojenie presmerovať na IP adresu daného webservera, v tomto prípade na adresu 192.168.1.2.



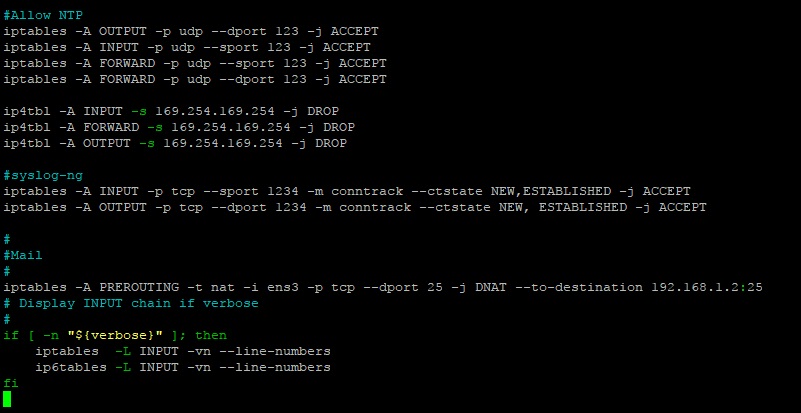
Obrázok 3 firewall - ICMP, DHCP, SSH, APACHE

Na obrázku 4vidíme sekciu NAT port forward, ktorá slúži na prekladanie verejnej IP adresy na lokálne. Následne v sekcii SSH tunnels smerujeme spojenia prichádzajúce na TCP port 1112 na IP adresu 192.168.1.2 pridanú stroju server 1 na TCP port 22 a spojenia prichádzajúce na TCP port 1113 na IP adresu 192.168.1.3, ktorá patrí stroju server 2, taktiež na TCP port 22. Tieto povolenia sú aplikované na rozhranie ***ens3***, čiže na rozhranie pripojené do internetu. Týmto bolo povolené vzdialené pripojenie prichádzajúce aj z inej ako lokálnej siete. Sekcia Allow DNS slúži na presmerovanie premávky prichádzajúcej na TCP alebo UDP port 53 na IP adresu nášho DNS serveru 192.168.1.2, čiže na stroj ***server 1*** na TCP alebo UDP port 53.



Obrázok 4 firewall - NAT, SSH tunely, DNS

Na obrázku 5 vidíme sekciu Allow NTP, ktorá povoluje prijatie, odoslanie a preposielanie paketov na UDP porte 123, ktorý slúži službe ***NTP***. V tejto sekcii sa taktiež zahadzujú pakety z IP adresy 169.254.169.254. Ide o cloud adresu, ktorá by potencionálne mohla spôsobiť zmeny v konfigurácii a toto opatrenie tejto možnosti zabráni. Sekcia syslog-ng slúži na otvorenie TCP portu 1234 a povoľuje príchod a odoslanie syslog-ng správ. V sekcii Mail vidíme nastavenie presmerovania paketov prichádzajúcich na TCP port 25 rozhrania ***ens3*** na IP adresu 192.168.1.2 nášho stroja server 1 na TCP port 25. Ide o port na ktorom pracuje mailová služba.



Obrázok 5 firewall - NTP, syslog, Mail

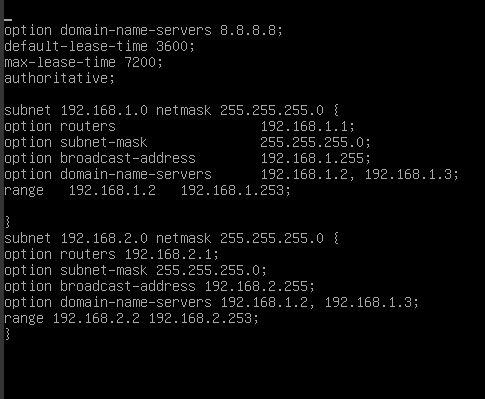
## **DHCP**

Služba DHCP slúži na prideľovanie voľných IP adries strojom, ktoré nemajú IP adresu zadanú staticky.

V prvom kroku je potrebné nainštalovať balíček isc-dhcp-server na stroji, ktorý bude slúžiť ako DHCP server. V našom prípade ide o ***server 1*** s IP adresou 192.168.1.2.

Inštaláciu balíčka spustíme príkazom apt-get install isc-dhcp-server.

Po nainštalovaní je potrebné pozmeniť konfiguračný súbor nachádzajúci sa na /etc/dhcp/dhcp.d. Náš konfiguračný súbor možno vidieť na obrázku 6.



Obrázok 6 dhcp.d

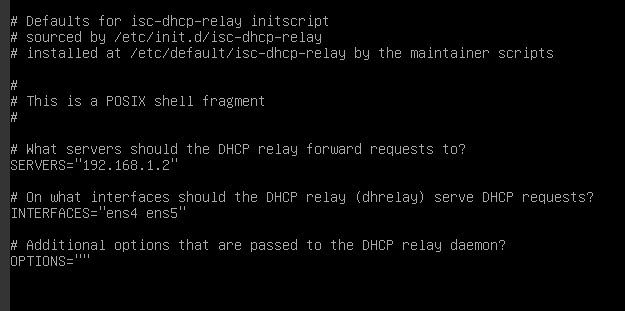
Na obrázku 6 vidíme základné informácie ako napríklad ***defaultný DNS server*** ukazujúci na známu IP adresu 8.8.8.8. Hodnoty default-lease-time a max-lease-time udávajú hodnoty koľko budú dané IP adresy prepožičané pred ich vypršaním. Ďalej je náš server nastavený ako authoritative.

Ďalšie časti súboru ukazujú vytvorenie 2 rozsahov sietí. Keďže klientská stanica sa nachádza v sieti 192.168.2.0/24 a servery sa nachádzajú v sieti 192.168.1.0/24, je nutné zadať rozsahy podľa strojov, ktoré budú o IP adresu žiadať.

Pre každý rozsah sa preto informácie môžu líšiť. Rozoberme si rozsah 192.168.1.0. Možnosť router udáva IP adresu pre default gateway. V našom prípade ide o rozhranie server-routra a tak adresu 192.168.1.1. Možnosť subnet-mask udáva masku, ktorú bude náš DHCP server rozdávať. Táto hodnota je nastavená na /24, čiže 255.255.255.0. Možnosť broadcast-address udáva poslednú adresu siete, ktorá predstavuje broadcastovú adresu, a tak v tomto prípade 192.168.1.255. Možnosť domain-name-server udáva IP adresy našich DNS serverov. V sieti máme 2, jeden hlavný a druhý záložný, no posielame ich obe IP adresy v prípade výpadku jedného z nich. Posledná možnosť range udáva rozsah adries ktoré budeme ponúkať. Ide o adresy z rozdahu 192.168.1.2 až 192.168.1.253.

Po tomto nastavení je server plne funkčný, avšak je nutné nastavenie DHCP relay na server-routri, aby sme vedeli prichádzajúce DHCP request správy zo siete 192.168.2.0/24 smerovať rozhraním až ku DHCP serveru. Preto je nutná inštalácia balíčku dhcp relay agent pomocou príkazu apt-get install isc-dhcp-relay.

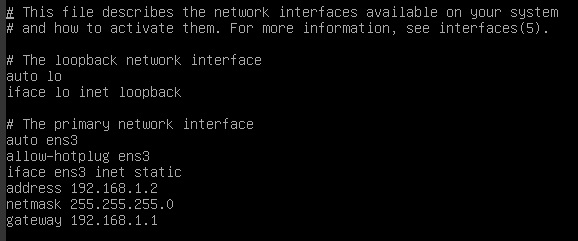
Po nainštalovaní je potrebné pozmeniť súbor /etc/default/isc-dhcp-relay nasledovne.



Obrázok 7 isc-dhcp-relay

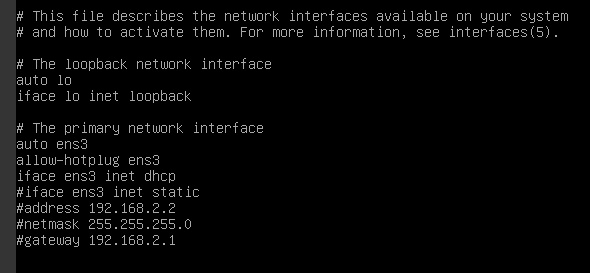
Pozmenili sme 2 riadky a to presnejšie SERVERS a INTERFACES. Do kolónky servers je nutné zadať IP adresu DHCP serveru, v našom prípade teda 192.168.1.2 a rozhranie cez ktoré sa k danému serveru dostaneme. V tomto prípade sme zadali obe rozhrania do lokálnej siete a to ens4 a ens5. DHCP server sa síce nachádza na rozhraní ens4, chceli sme ale ukázať aj možnosť zadania viacerých rozhraní.

Po tomto kroku máme funkčný ako samotný DHCP server tak aj DHCP relay. Už bolo nutné len nastavenie rozhraní samotných strojov. Pre stroje server sme chceli na rozhraniach statické IP adresy a tak sme do súboru /etc/network/interfaces zadali v prípade potrebnej statickej adresy nasledovné údaje (v tomto prípade ide o rozhranie ens3 na stroji server 1). Zadali sme IP adresu staticky a všetky potrebné údaje k tomu.



Obrázok 8 statická IP adresa

V prípade, že chceme adresu žiadať od DHCP servera je v tomto súbore nutné zadať namiesto slova static slovo dhcp a ostatné údaje nie sú potrebné. Na nasledujúcom obrázku je konfigurácia rozhrania ens3 pre stroj klient. Vidíme, že všetky ostatné údaje sú zakomentované a pýtame si IP adresu len od DHCP servera.



Obrázok 9 nastavenie klienta na DHCP

Týmto je DHCP konfigurácia ukončená.

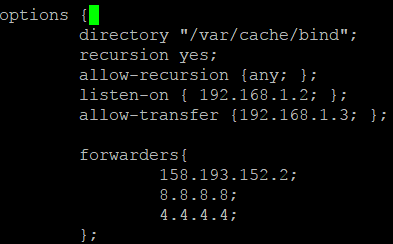
## **DNS**

Systém názvov domén, systém mien domén alebo systém doménových mien (Domain Name System), skr. DNS, je systém, ktorý ukladá prístup k informácii o názve stroja (hostname) a názve domény v istej distribuovanej databáze v počítačových sieťach ako internet. Najdôležitejšie je, že poskytuje mechanizmus získania IP adresy pre každé meno stroja (lookup) a naopak (reverse), a uvádza poštové servery (MX záznam) akceptujúce poštu pre danú doménu.

DNS poskytuje na internete všeobecne dôležitú službu, pretože kým počítače a sieťový hardvér pracujú s IP adresami, ľudia si vo všeobecnosti ľahšie pamätajú mená strojov a domén pri použití napr. v URL a e-mailovej adrese (obzvlášť nepríjemné by to bolo pri IPv6 adrese). DNS tak tvorí prostredníka medzi potrebami človeka a softvéru.

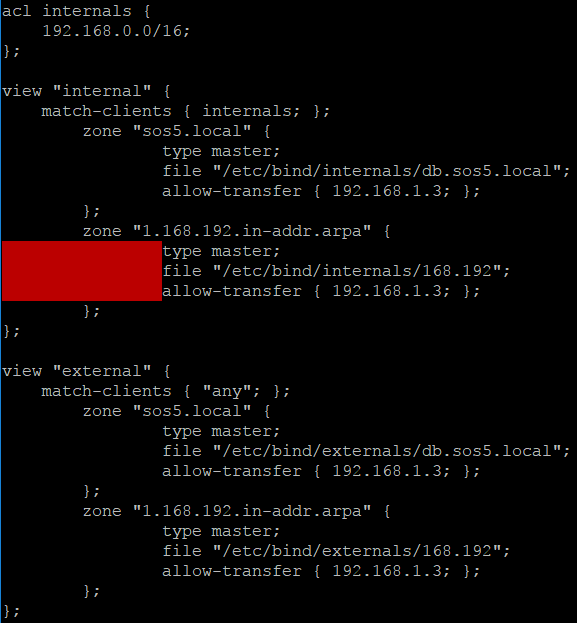
Na inštaláciu DNS servera je potrebné nainštalovať balíky bind9 a bind9-utils. Ako DNS master sme si zvolili server 1 a ako DNS slave sme zvolili server 2. Server 1 spravuje zónu sos5.cc.uniza.sk (avšak na obrázkoch je písaná zóna sos5.local, ktorú sme použili pri testovaní funkčnosti).

V konfiguračnom súbore /etc/bind/named.conf.options sme pridali do forwarders IP adresy 158.193.152.2, 8.8.8.8, 4.4.4.4 a povolili sme transfer zónových súborov na IP adresu serveru 2 (192.168.1.2).



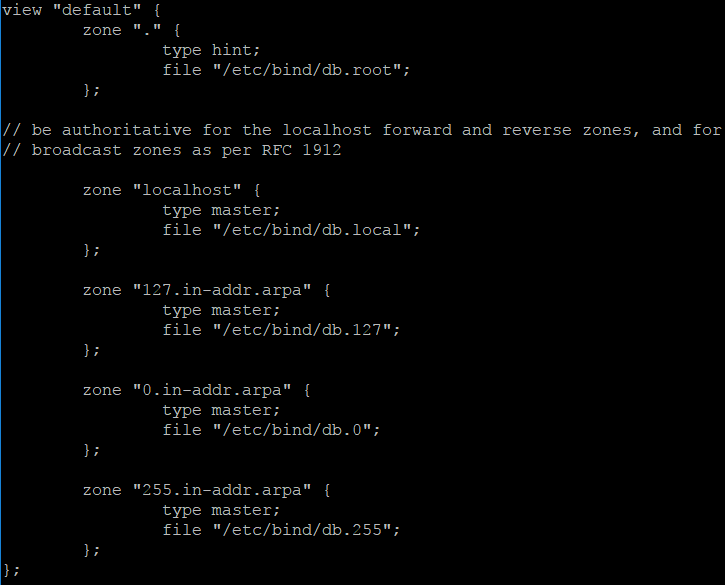
Obrázok 10 DNS - named.conf.options

Následne sme vytvorili dva pohľady, ktoré budú zabezpečovať vybavovanie dotazov z vonkajšej a internej časti siete. Tieto pohľady (views) boli vytvorené v súbore /etc/bind/named.conf.local. Na rozpoznanie klientov z internej siete sme vytvorili acl internals, ktorý obsahuje adresy používané v internej sieti.



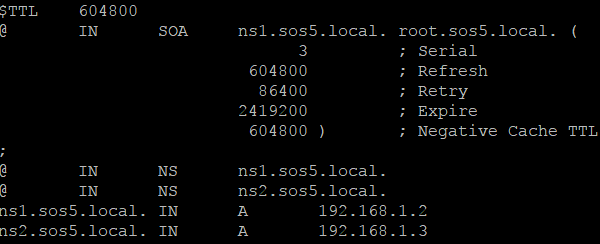
Obrázok 11 DNS - named.conf.local

Pravidlom je, aby sa každá zóna nachádzala v určitom pohľade. Z tohto dôvodu bol modifikovaný súbor /etc/bind/named.conf.default-zones.

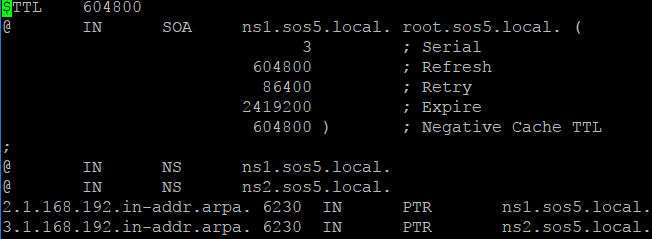


Obrázok 12 DNS - named.conf.default-zones

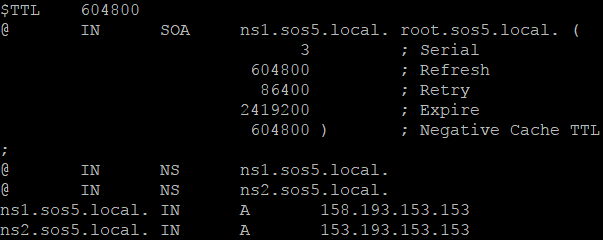
Pre jednotlivé pohľady sme si vytvorili zónové súbory, ktoré sa nachádzajú v nami vytvorených adresároch: /etc/bind/internals – pre internú zónu a /etc/bind/externals – pre externú zónu. Súbor db.sos5.local je určený pre vnútornú časť siete a 168.192 pre reverse DNS.



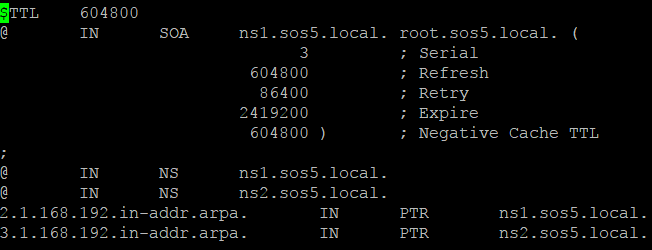
Obrázok 13 DNS - zónový súbor pre lokálnu časť siete



Obrázok 14 DNS - súbor 168.192



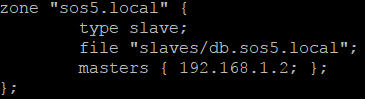
Obrázok 15 DNS - zónový súbor pre verejnú časť siete



Obrázok 16 DNS - súbor 168.192 pre verejnú časť siete

Slave si tieto súbory stiahne od mastera v binárnom tvare.

Na serveri 2 nainštalujeme bind rovnakým spôsobom ako na serveri 1. Pridáme zónu do súboru named.conf.local, nastavíme jej typ slave a IP adresu mastera (192.168.1.2).



Obrázok 17 DNS - slave named.conf.local

Firewall bol nakonfigurovaný tak, aby prepúšťal DNS požiadavky na lokálnej sieti, a tiež aby prepúšťal požiadavky z internetu na obidva DNS servery t.j. aby boli obidva DNS servery viditeľné zvonku (PREROUTING). Záznamy pre DNS sú pre verejnú IP adresu pre UDP aj TCP port 53 (zdrojový aj cieľový).

V prípade, že sa vyskytli problémy, skúšali sme vypnúť firewall, kontrolovali sme konfiguračné súbory Master DNS servera príkazmi named-checkconf, named-checkzone a príkazom tcpdump sme monitorovali prenášané správy.

Týmto bola ukončená konfigurácia služby DNS.

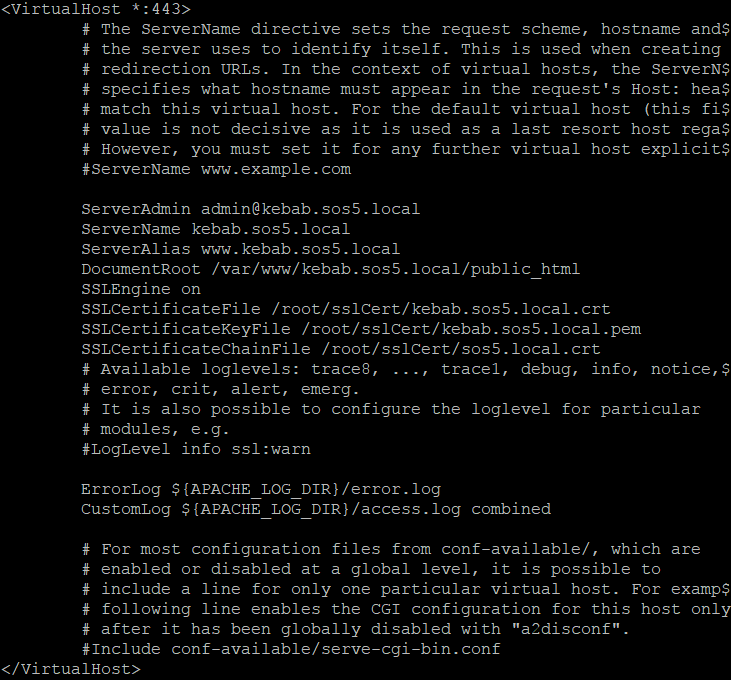
## **APACHE**

Apache HTTP Server je softwarový webový server s Opensource licenciou pre Linux, BSD, Microsoft Windows a iné platformy.

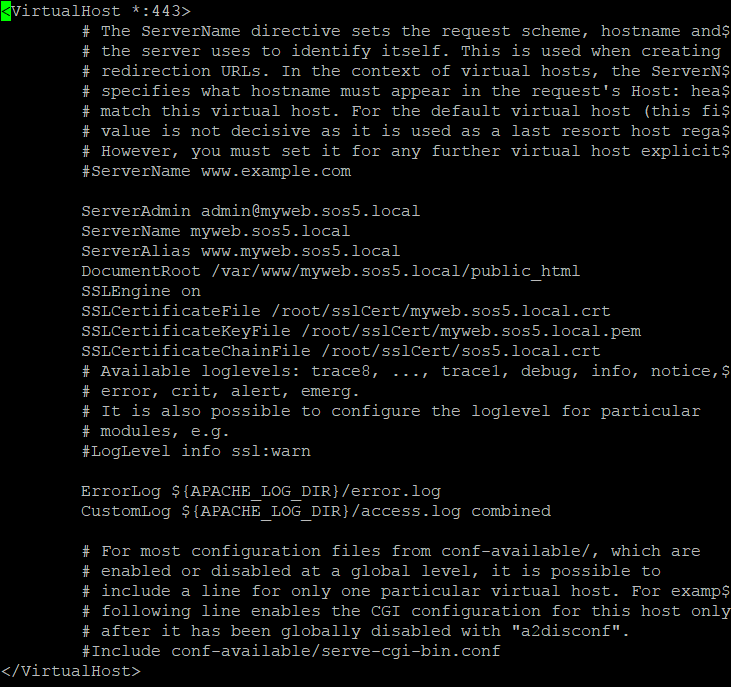
Ištalácia apache je pomerne jednoduchá, po updatnuti repozitára (príkaz apt-get update) si nainštalujeme apache 2 príkazom apt-get install apache2.

Na začiatok sme si pomocou programu xca vygenerovali SSL certifikáty, ktoré sme vložili do priečinku /root/sslCert. Následne bolo potrebné povoliť ssl príkazom a2enmod ssl.

V priečinku /etc/apache2/sites-aviable si vytvoríme 2 virtual host konfiguračné súbory pre naše stránky (kebab.sos5.local.conf a myweb.sos5.local.conf). V týchto súboroch sa nachádza viacero parametrov, ako napríklad názov stránky, cesta k súborom webstránky, povolenie SSL, a cesty k SSL certifikátom.



Obrázok 18 Apache – virtual host súbor



Obrázok 19 Apache – virtual host súbor

V priečinku /var/www sme si vytvorili 2 priečinky pre naše stránky kebab.sos5.locala myweb.sos5.local, do týchto priečinkov sme vytvorili priečinky public\_html a do nich súbory index.html do ktorých sme vložili text na rozpoznanie týchto dvoch stránok.

Následne do DNS záznamov sme museli pridať:



Obrázok 20 interné DNS

Do súboru /etc/bind/internals/db.sos5.local pre interný pohľad.

A



Obrázok 21 externé DNS

Do súboru /etc/bind/externals/db.sos5.local pre externý pohľad.

Do firewallu bolo potrebné pridať presmerovanie portov 443 a 80 na server 1. Tieto pravidlá sme pridali do scriptu pre náš firewall a bližšie sú popísané v predchádzajúcej kapitole o konfigurácii Firewallu.

Pre overenie kofigurácie sme použili príkaz - apache2ctl configtest.

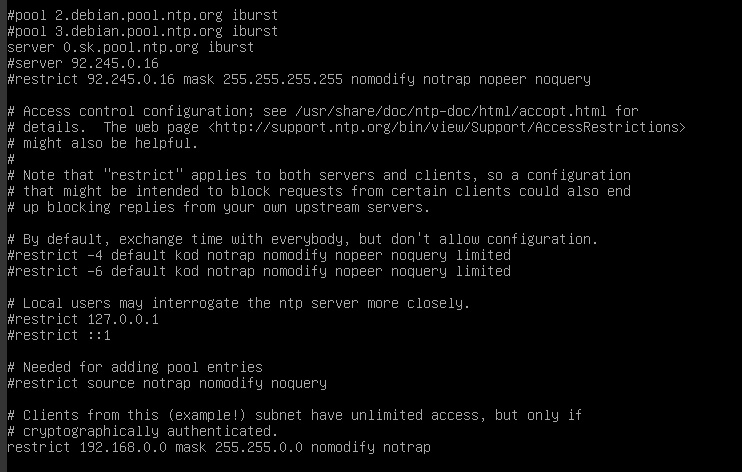
Následne sme znovu načítali konfiguráciu- service apache reload.

Týmto bola konfigurácia služby Apache ukončená.

## **NTP**

Služba NTP slúži na synchronizáciu hodín. V našom prípade sme si ako server vhodný pre túto službu vybrali server2 s IP adresou 192.168.1.3.

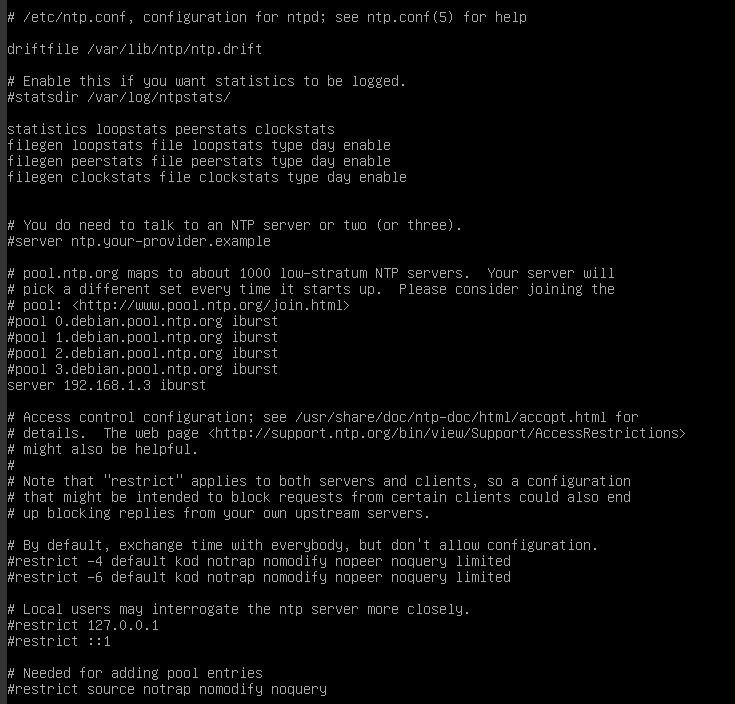
V prvom rade je potrebné nainštalovať službu pomocou príkazu apt-get install ntp. Po inštalácii sa vytvorí konfiguračný súbor /etc/nano.conf, ktorý je možné ďalej upravovať. Náš konfiguračný súbor serveru je možné vidieť na obrázku 20.



Obrázok 22 NTP - kofigurácia serveru

Ako si môžete všimnúť, odkomentované časti popisujú server podľa ktorého sa náš server bude nastavovať a potom len obmedzenie siete. V tomto prípade sme vybrali slovenský NTP server, ktorého meno ako aj IP adresa je dostupná na internete a prístup na náš NTP server sme obmedzili len pre sieť 192.168.0.0/16, keďže naša topológia obsahuje siete 192.168.1.0/24 a 192.168.2.0/24 a tento server slúži na obsluhu strojov v oboch týchto sieťach. V príkaze pre obmedzenie siete je taktiež parameter nomodify, ktorý zabraňuje zmene konfigurácie z iného stroja. Po zmene týchto nastavení je nutné reštartovať službu pomocou príkazu service ntpd restart.

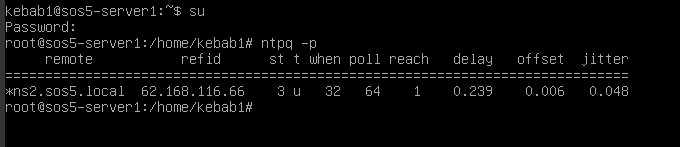
Pre klientské stanice je postup inštalácie rovnaký, ide len o iné zmeny v danom konfiguračnom súbore. Konfiguračný súbor serveru1 je možné vidieť na obrázku 21.



Obrázok 23 NTP - konfigurácia klienta

V tomto prípade sú zakomentované všetky defaultné NTP servery a namiesto toho je nastavená IP adresa nášho NTP serveru. Toto spôsobí, že server2 sa po novom bude snažiť zosynchronizovať s IP adresou 192.168.1.3, čiže s našim NTP serverom.

Kontrolu prevedieme pomocou príkazu ntpq –p na klientskej stanici.



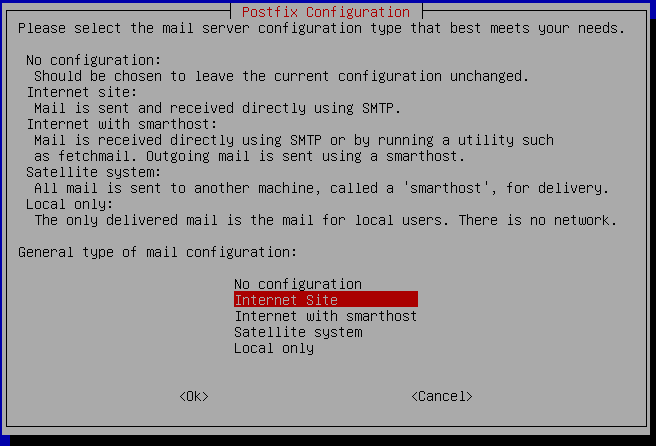
Obrázok 24 NTP - úspešná synchronizácia

Na obrázku 22 vidíme výpis na serveri1. Ukazuje synchronizáciu voči serveru ns2.sos5.local, čiže voči nášmu serveru 2.

Týmto je konfigurácia NTP ukončená.

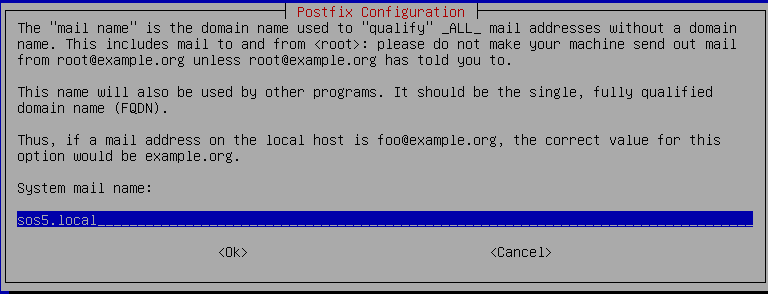
## **Mail**

Začneme inštaláciou balíčku mailutils pomocou príkazu apt-get install mailutils. Tento balíček obsahuje nástroje potrebné na testovanie. Následne nainštalujeme postfix a dovecot pomocou príkazu apt-get install postfix postfix-mysql dovecot-core dovecot-imapd dovecot-lmtpd dovecot-mysql. (je potrebné mať nainštalované mysql - apt get install mysql-server). Počas inštalácie sa nám zobrazí konfiguračná obrazovka, tu vyberieme možnosť internet site (obr. 25).



Obrázok 25 inštalácia postfix

Ďalej vyplníme doménové meno (sos5.local), čím sa ukončí inštalácia.



Obrázok 26 inštalácia postfix

Následne si pridáme do DNS MX záznam:

sos5.local. IN MX 10 ns1.local.

Pre použitie s SSL je potrebné vygenerovať si SSL certifikát, podobným spôsobom ako pri apache certifikátoch (certifikát generujeme pre mail server teda pre ns1.sos5.local).

Ďalej si vytvoríme mysql databázu pre náš mail server mysqladmin -p create servermail. Prihlásime sa do mysql mysql -u root -p a vytvoríme si používateľa pre mailserver príkazom GRANT SELECT ON servermail.\* TO 'usermail'@'127.0.0.1' IDENTIFIED BY 'heslo pouzivatela'; a príkazom FLUSH PRIVILEGES; sa uistíme že sú zmeny aplikované. Prepneme sa do databázy pomocou USE servermail; a vytvoríme si potrebné tabuľky pomocou nasledujúcich sql príkazov:

CREATE TABLE `virtual\_domains` (

`id` INT NOT NULL AUTO\_INCREMENT,

`name` VARCHAR(50) NOT NULL,

PRIMARY KEY (`id`)

) ENGINE=InnoDB DEFAULT CHARSET=utf8;

CREATE TABLE `virtual\_users` (

`id` INT NOT NULL AUTO\_INCREMENT,

`domain\_id` INT NOT NULL,

`password` VARCHAR(106) NOT NULL,

`email` VARCHAR(120) NOT NULL,

PRIMARY KEY (`id`),

UNIQUE KEY `email` (`email`),

FOREIGN KEY (domain\_id) REFERENCES virtual\_domains(id) ON DELETE CASCADE

) ENGINE=InnoDB DEFAULT CHARSET=utf8;

CREATE TABLE `virtual\_aliases` (

`id` INT NOT NULL AUTO\_INCREMENT,

`domain\_id` INT NOT NULL,

`source` varchar(100) NOT NULL,

`destination` varchar(100) NOT NULL,

PRIMARY KEY (`id`),

FOREIGN KEY (domain\_id) REFERENCES virtual\_domains(id) ON DELETE CASCADE

) ENGINE=InnoDB DEFAULT CHARSET=utf8;

Do tabuľky virtual\_domains si vložíme našu doménu (sos5.local) a FQDN serveru (ns1.sos5.local)

INSERT INTO `servermail`.`virtual\_domains`

(`id` ,`name`)

VALUES

('1', 'example.com'),

('2', 'hostname.example.com');

Pre testovacie účely si vytvoríme dvoch používateľov.

INSERT INTO `servermail`.`virtual\_users`

(`id`, `domain\_id`, `password` , `email`)

VALUES

('1', '1', ENCRYPT('heslo1', CONCAT('$6$', SUBSTRING(SHA(RAND()), -16))), 'email1@sos5.local'),

('2', '1', ENCRYPT('heslo2', CONCAT('$6$', SUBSTRING(SHA(RAND()), -16))), 'email2@sos5.local');

Ukončíme prácu s MYSQL pomocou príkazu exit. V súbore /etc/postfix/main.cf .si nastavíme cestu našim SSL certifikátom, teda upravíme prametre smtpd\_tls\_cert\_file a smtpd\_tls\_key\_file kde pôjdu (postupne) cesty k .pem a .key súborom. Všetky ostané parametre začínajúce smtpd\_tls zakomentujeme, okrem parametru smtpd\_use\_tls=yes a prídáme riadok smtpd\_tls\_auth\_only = yes ktorý vynúti použitie SSL na autorizáciu. Následne prídáme riadky:

smtpd\_sasl\_type = dovecot

smtpd\_sasl\_path = private/auth

smtpd\_sasl\_auth\_enable = yes

smtpd\_recipient\_restrictions =

permit\_sasl\_authenticated,

permit\_mynetworks,

reject\_unauth\_destination

Zmeníme parameter mydestination, aby obsahoval iba localhost a nastavíme parameter myhostname na naše FQDN, teda ns1.sos5.local. Pridaním týchto riadkov povolíme posielanie pošty na virtuálne domény ktoré sa nachácdzajú v MYSQL tabuľke a nakonfigurujeme postfix na prácu s virtuálnymi doménami, používateľmi a aliasmi:

virtual\_transport = lmtp:unix:private/dovecot-lmtp

virtual\_mailbox\_domains = mysql:/etc/postfix/mysql-virtual-mailbox-domains.cf

virtual\_mailbox\_maps = mysql:/etc/postfix/mysql-virtual-mailbox-maps.cf

virtual\_alias\_maps = mysql:/etc/postfix/mysql-virtual-alias-maps.cf

Ďalej si vytvoríme .cf súbory ktoré sme pridali do konfigurácie v predošlom kroku.

Súbor mysql-virtual-mailbox-domains.cf:

user = usermail

password = heslo pre usermail pouzivatela

hosts = 127.0.0.1

dbname = servermail

query = SELECT 1 FROM virtual\_domains WHERE name='%s'

Súbor mysql-virtual-mailbox-maps.cf:

user = usermail

password = heslo pre usermail pouzivatela

hosts = 127.0.0.1

dbname = servermail

query = SELECT 1 FROM virtual\_users WHERE email='%s'

A súbor mysql-virtual-alias-maps.cf:

user = usermail

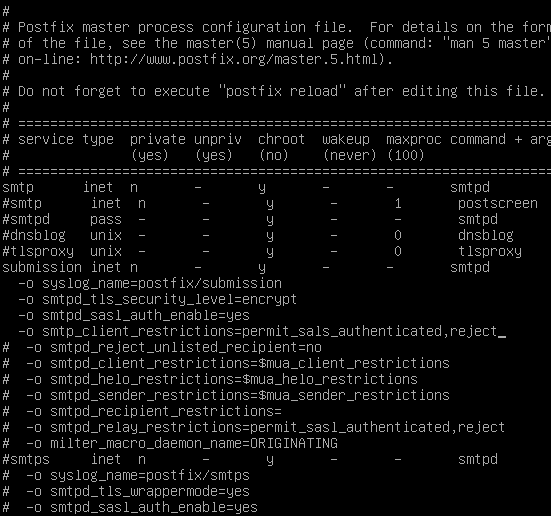
password = heslo pre usermail pouzivatela

hosts = 127.0.0.1

dbname = servermail

query = SELECT destination FROM virtual\_aliases WHERE source='%s'

Je potrebné povoliť port 587 pre bezpečné pripojenie s clientami. V súbore /etc/postfix/master.cf file odkomentujeme riadky a pridáme riadok -o smtpd\_client\_restrictions=permit\_sasl\_authenticated,reject tak aby náš súbor vyzeral ako súbor na obrázku 27.



Obrázok 27 master.cf

Nakoniec reštartujeme postfix príkazom service postfix restart. Začneme s konfiguráciou dovecotu v súbore /etc/dovecot/dovecot.conf, v tomto súbore pridáme riadok pre povolenie protokolov protocols = imap lmtp pop3, tak ako na obrázku 28.



Obrázok 28 dovecot.conf

V súbore /etc/dovecot/conf.d/10-mail.conf nastavíme (a prípadne odkomentujeme) parameter mail\_location = maildir:/var/mail/vhosts/%d/%n a parameter mail\_privileged\_group = mail. V priečinku /var/mail/ si vytvoríme priečinok vhosts, v ktorom vytvoríme prečinky pre všetky domény v mysql tabuľke (sos5.local a ns1.sos5.local). Vytvoríme používateľa a skupinu vmail (skupina bude mať id 5000).

groupadd -g 5000 vmail

useradd -g vmail -u 5000 vmail -d /var/mail

Ďalej nastavíme vlastníka priečinku /var/mail na nášho vytvoreného používateľa a skupinu. chown -R vmail:vmail /var/mail.

V súbore /etc/dovecot/conf.d/10-auth.conf vypneme plaintextovú autentifikáciu odkomentovaním riadku disable\_plaintext\_auth = yes. Ďalej zmeníme parameter auth\_mechanisms = plain na auth\_mechanisms = plain login a zakomentujeme riadok !include auth-system.conf.ext. Je potrebné povoliť mysql autorizáciu odkomentovaním riadku !include auth-sql.conf.ext. Súbor auth-sql.conf.ext následne vytvoríme a vložíme do neho:

passdb {

driver = sql

args = /etc/dovecot/dovecot-sql.conf.ext

}

userdb {

driver = static

args = uid=vmail gid=vmail home=/var/mail/vhosts/%d/%n

}

V súbore /etc/dovecot/dovecot-sql.conf.ext nastavíme (a prípadne odkomentujeme) parametre driver = mysql, connect = host=127.0.0.1 dbname=servermail user=usermail password=heslo na usermail, default\_pass\_scheme = SHA512-CRYPT a password\_query = SELECT email as user, password FROM virtual\_users WHERE email='%u';.

Zmeníme vlstníka a skupinu priečinku dovecot na vmail.

chown -R vmail:dovecot /etc/dovecot

chmod -R o-rwx /etc/dovecot

Upravíme súbor /etc/dovecot/conf.d/10-master.conf , aby vypadal nasledovne:

service imap-login {

inet\_listener imap {

port = 0

}

inet\_listener imaps {

}

}

service pop3-login {

inet\_listener pop3 {

#port = 110

}

inet\_listener pop3s {

#port = 995

#ssl = yes

}

}

service lmtp {

unix\_listener /var/spool/postfix/private/dovecot-lmtp {

mode = 0600

user = postfix

group = postfix

}

}

service imap {

}

service pop3 {

}

service auth {

unix\_listener /var/spool/postfix/private/auth {

mode = 0666

user = postfix

group = postfix

}

unix\_listener auth-userdb {

mode = 0600

user = vmail

}

user = dovecot

}

service auth-worker {

user = vmail

}

service dict {

unix\_listener dict {

}

}

Nakoniec v súbore /etc/dovecot/conf.d/10-ssl.conf nastavíme vynútenie ssl a cesty k ssl certifikátom zmenou prarametrov:

ssl = required

ssl\_cert = </root/sslCert/dovecot.pem

ssl\_key = </root/sslCert/dovecot\_key.pem

Po reštartovaní služby dovecot (service dovecot restart) môžeme overiť funkčnosť nášho mailserveru.

**Overenie funkčnosti**

Na overenie funkčnosti sme použili nasledovné príkazy:

postmap -q sos5.local mysql:/etc/postfix/mysql-virtual-mailbox-domains.cf – overenie či postfix nájde našu doménu.

postmap -q email1@sos5.local mysql:/etc/postfix/mysql-virtual-mailbox-maps.cf -overenie či postfix nájde emailovú adresu.

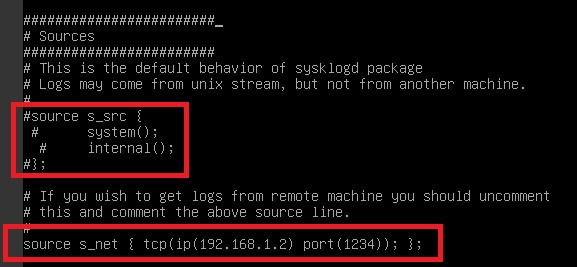
telnet sos5.local 993 – overenie portu 993

emailoveho klienta – overenie funkčnosti mail serveru (pripojenie na server, prihlásenie, poslanie správy, prijatie správy).

## **Syslog**

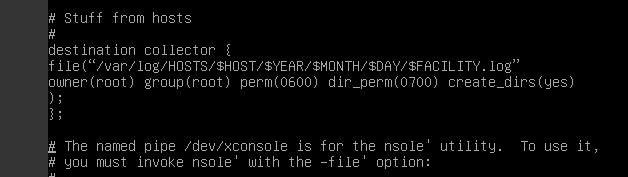
V prvom kroku je potrebné nainštalovať službu pomocou príkazu apt-get install syslog-ng. Po inštalácii je konfiguračný súbor uložený v /etc/syslog-ng/syslog-ng.conf. V našej práci sme si ako server pre zber dár vybrali server1 s IP adresou 192.168.1.2.

Ako vidíme na obrázku, ak chceme stroj využívať na zber logov, je potrebné zakomentovanie defaultného nastavenia zdroja a nastaviť IP adresu a port na ktorej stroj bude počúvať a zbierať logy.



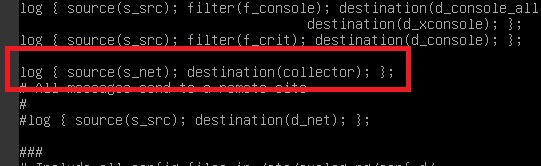
Obrázok 29 syslog-ng.conf

V nasledujúcom obrázku sme si vytvoritli takzvaný collector, ktorý po zbere správ vytvorí úložisko podľa názvu klienta, dátumu a služby ktorá sa logovala. Obsahuje aj nastavenie práv pre vytvorenie požadovaných súborov.



Obrázok 30 collector

V tomto prípade už máme nastavené čo a kde treba ukladať, avšak je ešte potrebné tieto dve časti spojit. To môžeme vidieť na nasledujúcom obrázku.

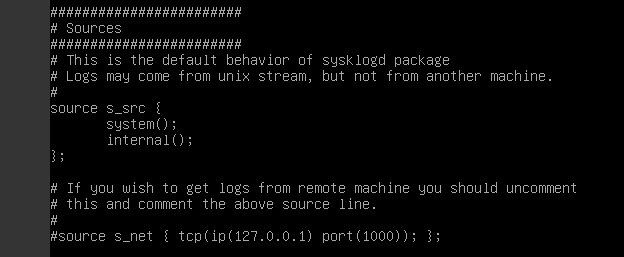


Obrázok 31 s\_net

Naďalej je možné v službe syslog-ng presnejšie upresňovať filtre a služby ktoré sa majú logovať, pre jednoduchosť riešenia sme tieto možnosti vynechali. Logujú sa defaultné služby a uchovávajú alebo posielajú sa defaultne nastavené úložiská.

Týmto je konfigurácia na strane servera ukončená. Prejdime teda na konfiguráciu klientskej stanice. Je taktiež nutné nainštalovanie balíčka a prístup do konfiguračného súboru.

Pre ukážku konfigurácie klientskej stanice sme vybrali server-router. Ako vidíme na obrázku, ponechali sme logovanie defaultných logov.

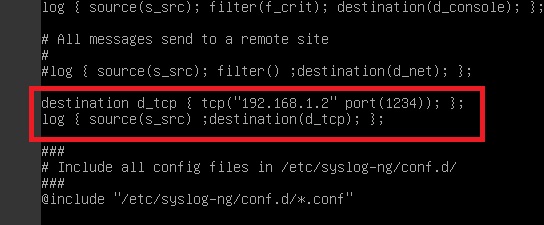


Obrázok 32 s\_src

V tomto prípade je možné určenie ciest pre logovanie špecifických súborov. Pre zalogovanie súboru je nutné do s\_src dopísať napríklad file(“/var/log/myapplication.log“ follow-freq(1)) ;

Z dôvodu jednoduchosti ukážky sme bližšie nešpecifikovali presnejšie logovanie našich súborov.

V nasledujúcom obrázku vidíme nastavenie IP adresy 192.168.1.2 s portom 1234 ako cieľ pre naše logy. Ide o náš server1, ktorý sme pred chvíľkou konfigurovali. A taktiež môžeme vidieť spojenie nášho zdroja logov s daným cieľom.



Obrázok 33 d\_tcp

Po zmene konfigurácie či už na serveri alebo na klientskej stanici je nutné reštartovať službu príkazom service syslog-ng restart. Otváranie firewallu a iné zmeny sú bližšie popísané v kapitole Firewall.

# Windows

## **Topológia zapojenia**

Topológia SOS sa skladá z routera, dvoch serverov a klienta.

|  |  |  |  |
| --- | --- | --- | --- |
| Názov zariadenia | Rozhranie | IP adresa | Popis |
| Server-router | Ethernet  Ethernet  Ethernet 2  Ethernet 3 | 158.193.153.235  158.193.153.249  192.168.1.1  192.168.2.1 | Windows server 2016 |
| Server1 | Ethernet | 192.168.1.2 | Windows server 2016 |
| Server2 | Ethernet | 192.168.1.3 | Windows server 2016 |
| Klient | Ethernet | DHCP | Windows desktop |

*Tabuľka 2 Adresný plan Windows*

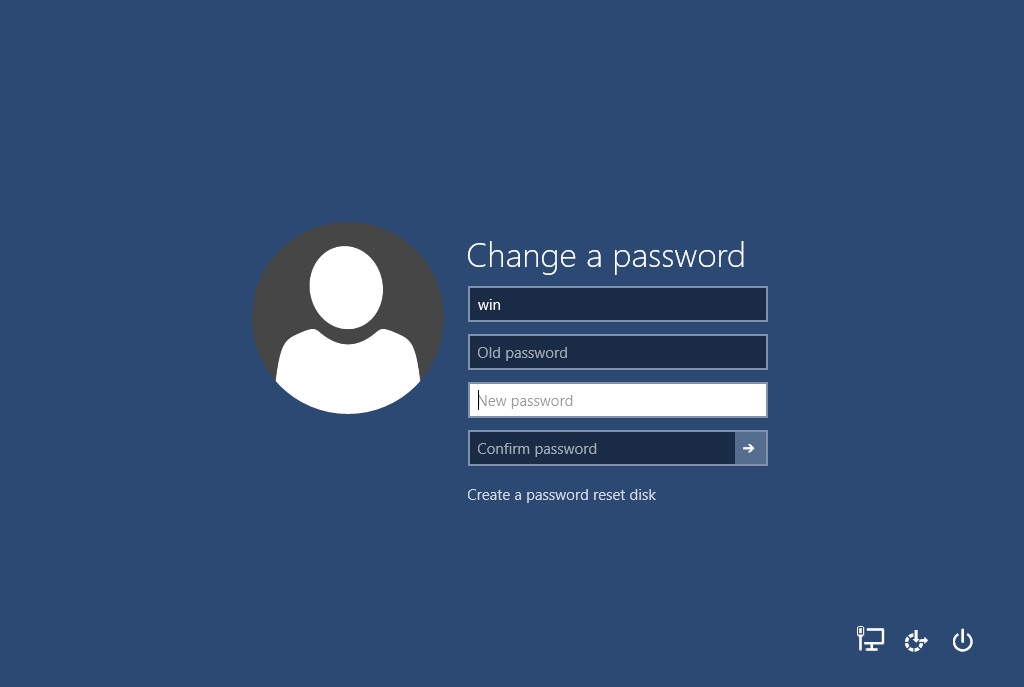
Druhá časť projektu sa skladá z nasadenia určených služieb na rovnakú sieť ako v prvej časti, avšak s použítím strojov so systémom Windows. Taktiež sú určené nové IP adresy pre DNS zóny tejto siete.

1. ns1.sos5.cc.uniza.sk: 158.193.153.149
2. ns2.sos5.cc.uniza.sk: 158.193.153.153

## **Základná konfigurácia**

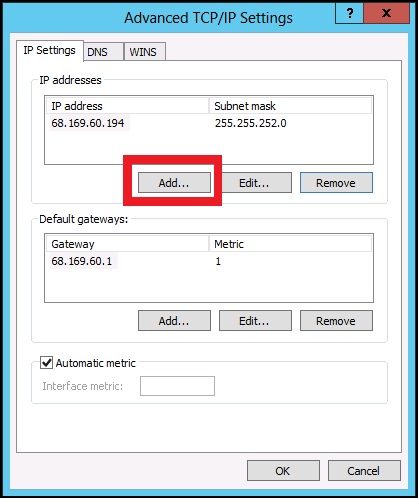
Základná konfigurácia pozostávala z nastavenia hesiel pre prihlasovacie kontá a z nastavenia požadovaných IP adries rozhraniam.

Nastavenie nového hesla pre účet dosiahneme skratkou Ctrl+Atl+Del, otvoríme ponuku v ktorej sa nám zobrazí možnosť Change password. V tomto kroku si od nás systém vypýta staré heslo a 2x nové, ako je možné vidieť na obrázku. Po potvrdení bolo heslo úspešne zmenené.



Obrázok 34 zmena hesla Windows

Nastavenie IP adries je možné pomocou Network and Sharing Center, kde vyberieme možnosť Change adapter settings, vyberieme rozhranie a prejdeme do jeho vlastností. Vyberieme možnosť Internet Protocol Version 4 a znovu prejdeme do vlastností. V tomto kroku je možné nastavenie buď DHCP alebo statickej IP adresy. V prípade potreby 2 IP adries pre jedno rozhranie ako je tomu pri stroji server-router, prejdeme na možnosť Advanced. V tomto okne je možné priradenie viacerých IP adries jednému rozhraniu ako je zobrazené na obrázku.



Obrázok 35 Pridanie viacerých IP adries Windows

Strojom tak boli nastavené požadované adresy a heslá.

Týmto bola ukončená základná konfigurácia.

## **DHCP**

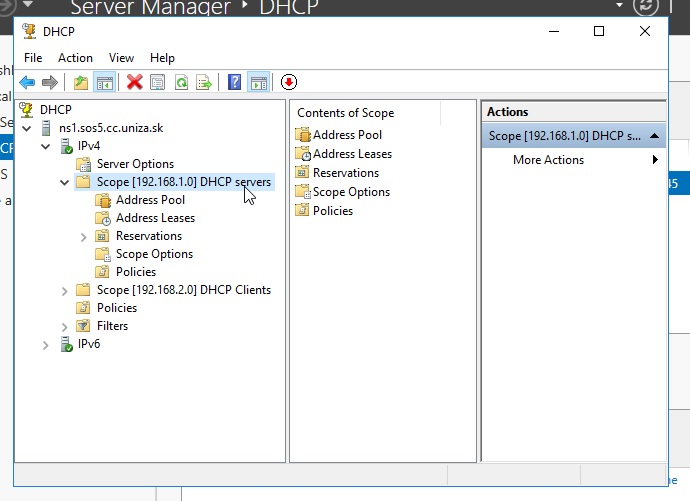
Inštalácia prebehla pomocou Windows service manager výberom možnosti Add Roles and Features a pod kartou Server Roles sme vybrali DHCP Server, ktorý sme následne nainštalovali.

Po nainštalovaní služby sme prešli do DHCP Manager kde sme vybrali IPv4 a vytvorili 2 nové rozsahy. Rozsah je nutné vytvoriť 2x, pretože chceme obsluhovat klienta v inej sieti a pre neho je potrebné ponúkať IP adresy z inej siete.

Pri vytváraní rozsahu nás systém požiada o zadanie mena, následne o zadanie rozsahu IP adries a potom o možnosť zadania adries, ktoré síce do rozsahu patria ale nebudú sa ponúkať. Pred koncom konfigurácie je nutné nastavenie aj dĺžky pamätania si rozdaných adries. V našom prípade sme tento limit nastavili na 30 dní. V poslednom kroku sa server opýta či chceme nastaviť aj potrebné DNS a default gateway adresy pre daný rozsah. V tomto prípade je možnosť tento krok preskočiť a nakonfigurovať neskôr. My sme avšak zvolili konfiguráciu ihneď a ako DNS adresu sme pridali adresu serveru2, ktorý v našej topológii slúži aj ako DNS server a ako gateway adresu sme pridali adresu portu spojeného s našim server-routrom podľa potreby daného rozsahu.

**Vytvorene boli nasledovné**:

1. Rozsah s názvom DHCP servers so štartovacou IP adresou 192.168.1.2 a s poslednou adresou 192.168.1.254 a s maskou 255.255.255.0. Taktiež boli z rozsahu odobrané adresy 192.168.1.2 a 192.168.1.3, pretože ide o adresy našich serverov ktoré sme nastavili staticky. DNS adresa bola nastavená na IP adresu serveru2 a to 192.168.1.3 a adresa default gateway bola nastavená na adresu 192.168.1.1.
2. Rozsah s nazvom DHCP clients so štartovacou IP adresou 192.168.2.2 a s poslednou adresou 192.168.2.254 a s maskou 255.255.255.0. DNS adresa bola nastavená na IP adresu serveru2 a to 192.168.1.3 a adresa default gateway bola nastavená na adresu 192.168.2.1.



Obrázok 36 DHCP rozsah Windows

Týmto bola konfigurácia DHCP ukončená, avšak bolo nutné na server-routri pomocou funkcie DHCP relay umožniť pridanie adries klientov zo siete 192.168.2.0/24.

Pre nakonfigurovanie DHCP relay je nutné v okne Server Manager -> Dashboard -> Tools prejsť na Remote Access Manager. Otvorí sa nám okno s názvom Remote Access Management Console, kde je následne nutné kliknúť na Direct Access and VPN a potom Open RRAS Management.

Otvorí sa nám okno s názvom Routing and Remote Access, kde máme v ponuke IPv4 a IPv6. Náš DHCP server ponúka IPv4 adresy a tak rozklikneme IPv4, klikneme pravým na General a vyberieme New Routing Protocol.

V tomto kroku už vidíme možnosť označenia DHCP Relay Agent, ktorý vyberieme. Pod kartu IPv4 sa nám pridá DHCP Relay Agent a môžeme pristúpiť ku samotnej konfigurácii. Preto klikneme pravým na DHCP Relay Agent a zvolíme Properties. Tu je potrebné nastaviť IP adresu nášho DHCP serveru. Vrátime sa do karty IPv4 ->DHCP Relay Agent, klikneme pravým a zvolíme New Interface. Toto nastavenie požaduje zvolenie rozhrania na ktorom nájdeme náš DHCP server. Vybrali sme teda rozhranie ktoré spája server-router so serverom2.

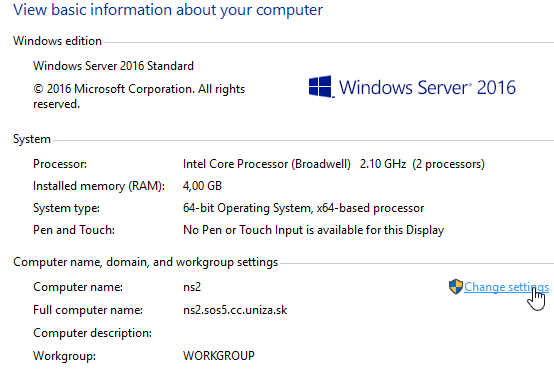
Týmto bola konfigurácia DHCP relay ukončená.

## **DNS**

Keďže windows DNS server nepodporuje pohľady ako BIND, rozhodli sme sa vytvoriť si dva DNS servery, jeden (server 2) pre interné DNS, a jeden (server 1) pre externé DNS.

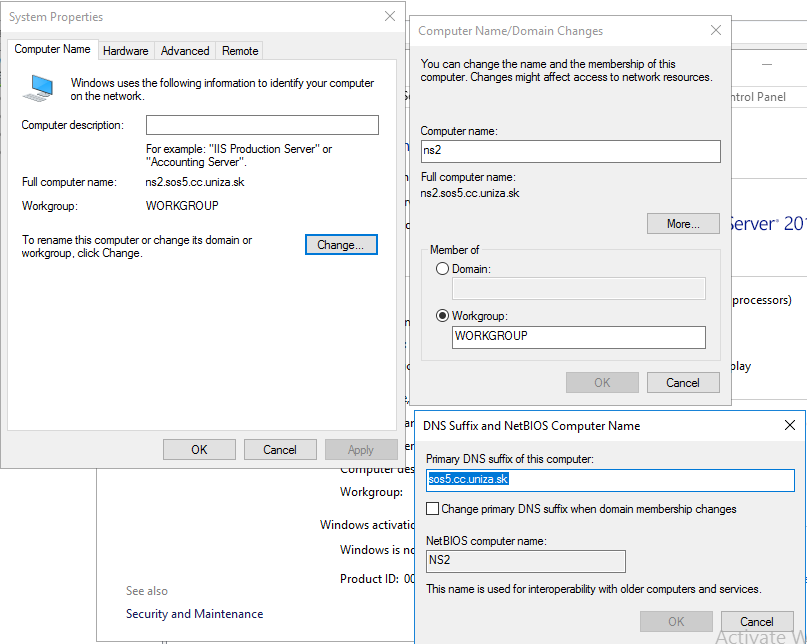
DNS server nainštalujeme pomocou Windows Server Managera. Klikneme na Manage , vyberieme možnosť Addroles and features*,* daľej Role-based or feature-based installation, zobrazí sa zoznam serverov, my vyberieme náš server a zvolíme zo zoznamu roles DNS Server a dokončíme inštaláciu.

Pred začatím konfigurácie DNS, je vhodné nastaviť si korektný hostname, a DNS suffix serveru (neskôr to môže robiť problémy). Otvoríme si ovládací panel. Následne ideme do nastavenia názvu počítača Control panel -> System and security -> System, v časti Computer name, domain and workgroup klikneme na change settings.



Obrázok 37 System

Zobrazí sa okno system properties kde v záložke Computer name klikneme na change. Následne sa zobrazí okno Computer name/Domain Changes, kde vyplníme názov počítača (sme na serveri 2, takže ns2). Klikneme na more a zobrazí sa okno pre vyplnenie DNS suffixu, kde zadáme doménové meno, bez názvu PC (sos5.cc.uniza.sk). Potvrdíme zmeny tlačidlom OK.

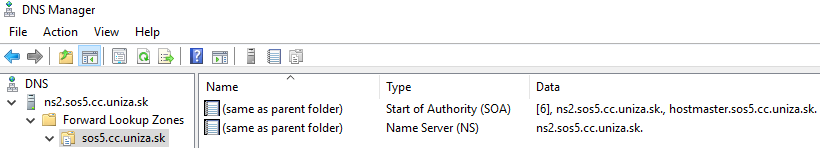


Obrázok 38 DNS suffix Windows

Pre prejavenie zmien je potrebné server reštartovať. Rovnako postupujeme aj na serveri.

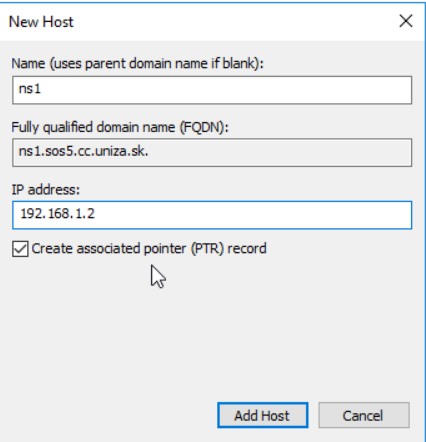
**Konfigurácia DNS**

Klikneme pravým na náš server a vyberieme možnosť new zone. Zobrazí sa okno sprievodcu vytvorením novej zóny. Vyberieme typ primary zone, forward lookup zone, napíšeme názov zóny (sos5.cc.uniza.sk), vyberieme možnosť vytvorenia zónového súboru, zakážeme dynamické updaty. Kliknutím na tlačidlo finish, sa nám vytvorí zóna ktorá obsahuje záznamy SOA, a NS záznam pre náš server.



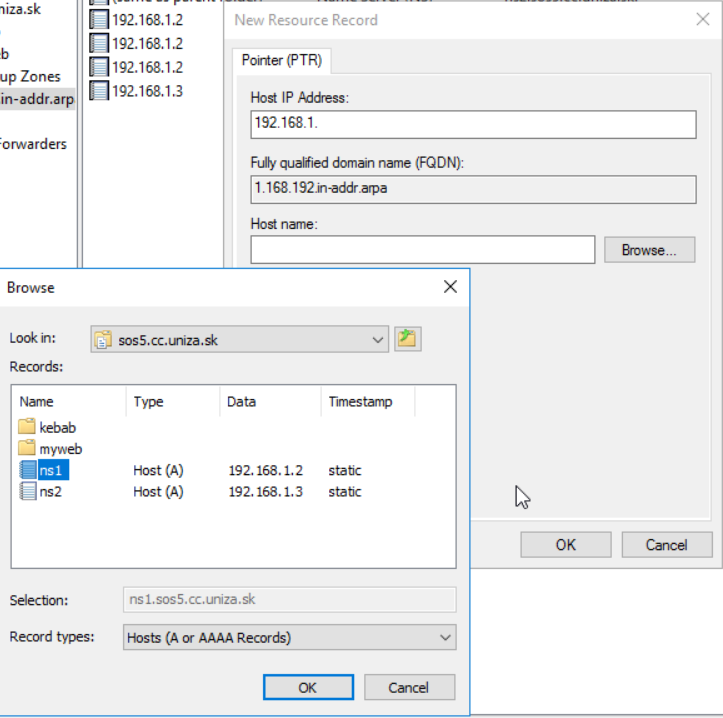
Obrázok 39 DNS Windows

Následne pridáme A záznamy pre server 1 a server 2. Klikneme pravým tlačidlom na zónu, vyberieme možnosť New Host(A or AAAA). Vyplníme položku name, kde zadáme . V poli FQDN si môžeme skontrolovať či je výsledné doménové meno servera korektné a následne vyplníme IP adresu serveru (pre interné DNS jeho súkromnú adresu a pre externé, verejnú adresu).



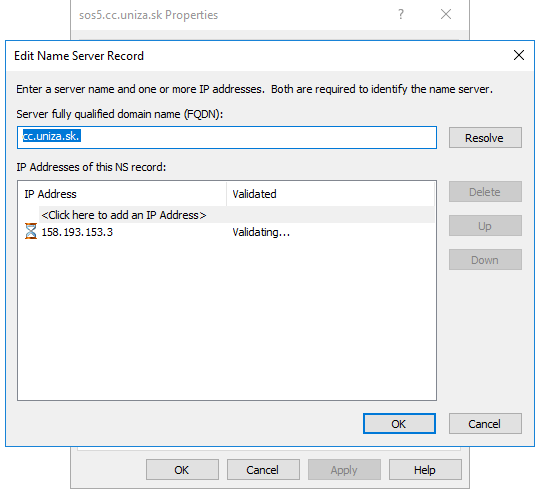
Obrázok 40 New host

Následne si pridáme záznamy do reverse looklup zóny. Klikneme pravý tlačidlom na reverznú zónu, vyberieme možnosť New Pointer (PTR), zobrazí sa nám dialógové okno, kde môžeme zadať potrebné údaje manuálne, alebo klikneme na tlačidlo browse a vyberieme záznam z našej zóny, po potvrdení sa vyplní hostname a ip adresa v potrebnom formáte.



Obrázok 41 New pointer

Ďalej pridáme autoritatívny nameserver pre naše DNS (v našom prípade nameserver pre zónu cc.uniza.sk). Klikneme pravým na zónu->properies zobrazíme záložku name servers, klikneme na tlačidlo add. Zobrazí sa okno na pridanie nového záznamu, kde zadáme IP adresu nášho autoritatívneho DNS serveru. Po validácií by sa malo zobraziť aj FQDN, klikneme na OK a potvrdíme zmeny. V zóne by sa mal následne objaviť NS záznam pre novo pridaný server.



Obrázok 42 Edit name server record

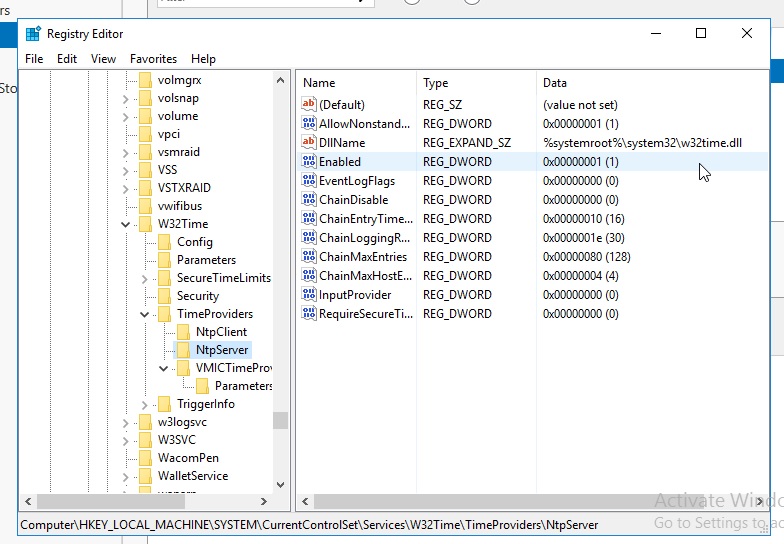
Podobne postupujeme aj na serveri 1, kde ale namiesto súkromných adries použijeme verejné adresy.

Vo firewalle bude potrebné otvoriť porty pre DNS, a aj vytvoriť presmerovanie portov z verejnej IP adresy na súkromnú IP adresu serveru 1, kde je naše verejné DNS. Presmerovanie docielime zadaním nasledovných príkazov:

* netsh routing ip nat portmapping “Ethernet2“ tcp 0.0.0.0 53 192.168.1.2 53
* netsh routing ip nat portmapping “Ethernet2“ udp 0.0.0.0 53 192.168.1.2 53

## **NTP**

Služna NTP pre Windows Server sa spúšťa pomocou editovania registrov. A preto sme skratkou Win+R otvorili Run okno, napísali regedit a prešli do zoznamu registrov. Je nutné nastaviť cestu HKEY\_LOCAL\_MACHINE -> SYSTEM -> CurrentControlSet -> Services -> W32Time -> TimeProviders -> NtpServera zmeniť hodnotu Enable z 0 na 1.



Obrázok 43 regedit NTP

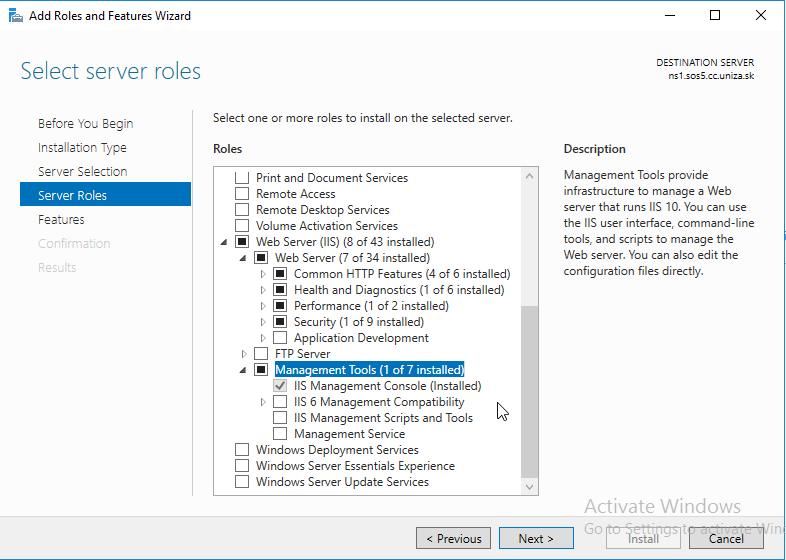
Ďalším krokom je spustenie NTP serveru pomocou zadania príkazu w32tm /config /update do okna Run, ktorý znovu otvoríme pomocou skratky Win+R.

Aktualizáciu zmien umožníme príkazom net stop w32time && net start w32time do príkazového riadku.

Týmto je konfigurácia služby NTP ukončená.

## **IIS – Internet Information Server**

Webserver IIS sme pridali cez windows server manager tlačidlom Add roles and features, kde sme v ponuke Server Roles vyhľadali Web Server (ISS) a pokračovali v inštalácií webserveru.



Obrázok 44 Add roles and features

Po úspešnej inštalácii sa IIS objaví na ľavom paneli v server manager-i. Klikneme na ikonu IIS a v zozname dostupných serverov sa zjaví jeden - ten, na ktorom uskutočňujeme konfiguráciu. Klikneme naň pravým tlačidlom myši a z ponuky zvolíme možnosť Internet Information Services (IIS) Manager. Otvorí sa nové okno, v ktorého ľavom paneli sa nachádza náš server. Rozbalíme jeho ponuku a klikneme na Sites. Pravý klik na Default Web Site nám ponúkne viacero možností vrátane nastavenia webstránky a pridania novej. Následne odstránime defaultnú stráku (pre náš účel je nepotrebná). Na disku serveru si vytvoríme priečinky pre naše webové stránky (v našom prípade C:\\kebab a C:\\myweb). Do priečinku vytvoríme súbory index.htm. Pre testovacie účely sme vytvorili súbory ktoré obsahovali text „kebab“ a „myweb“ aby sme vedeli rozlíšiť medzi stránkami.

Vrátime na naspäť do IIS managera, kde pridáme dve nové stránky (pravý klik na sites->Add website). Zobrazí sa nám dialógové okno pre pridanie novej stránky. V tomto okne vyplníme:

* názov stránky (v našom prípade myweb)
* cestu ku priečinku stránky (C:\\myweb)
* binding (u nás typ http a ip adresa serveru na porte 80) //potrebný edit pre https
* a hostname ([www.myweb.sos5.cc.uniza.sk](http://www.myweb.sos5.cc.uniza.sk))

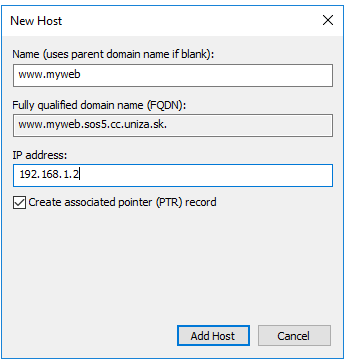
Následne rovnakým spôsobom pridáme druhú stránku.

**Úpravy v DNS**

Pre korektné fungovanie našich stránok je potrebné vykonať úpravy v konfigurícií DNS.

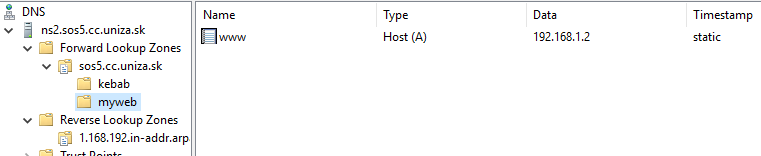
**Interné DNS:**

Otvoríme si DNS manager na serveri 2 (naše interné DNS). Pridáme dva nové a záznamy pre naše stránky. (klik pravým tlačidlom na zónu, New Host (A or AAAA)). Vyplníme položku name, kde zadáme www.nazovStranky (napr. www.myweb). V poli FQDN si môžeme skontrolovať či je výsledné doménové meno servera korektné a následne vyplníme súkromnú IP adresu serveru 1.



Obrázok 45 interný new host

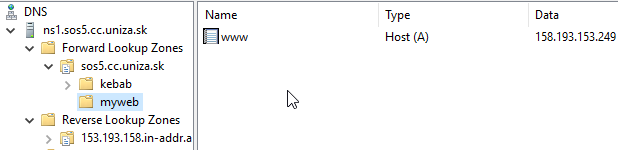
Vo výsledku bude naše interné DNS vyzerať takto:



Obrázok 46 interné DNS

**Externé DNS:**

Postupujeme rovnako ako pri internom DNS, s tým rozdielom, že namiesto internej IP adresy serveru 1 použijeme verejnú, alebo v našom prípade verejnú adresu server routeru, na ktorom následne nastavíme presmerovanie portov na server 1.



Obrázok 47 externé DNS

**Úpravy vo firewalle**

Pre korektné fungovanie našich stránok je potrebné vykonať úpravy v konfigurícií firewallu. Je potrebné otvoriť porty ako aj presmerovať pakety na stroji server-router pomocou príkazov použitých pri konfigurácii DNS. Avšak je potrebné zmeniť port v príkaze.

Týmto bola konfigurácia služby ISS ukončená.

# Záver

Prácou na týchto topológiach sme sa naučili spravovať viacero služieb, či už pre systém Linux alebo Windows server. Oboznámili sme sa s rozdielmi medzi danými systémami a ich implementáciou daných služieb. Počas vypracovania zadania sme narazili na viacero problémov, ktorých riešenia niekedy boli zdĺhavé, ale tieto poznatky budeme môcť aplikovať v budúcnosti pri práci a konfigurácii služieb aj pre iné systémy.